California State Public Policy

Advancing the Business of Technology

"FRAMING THE DISCUSSION"

TESTIMONY OF AeA – CALIFORNIA RADIO-FREQUENCY IDENTIFICATION DOCUMENT (RFID) HEARING – CALIFORNIA RESEARCH BUREAU

October 31, 2007

A. RFID – Privacy And Security Protections Depend On Risk To Privacy And Security.

While today's hearing is about RFID and government identifications, RFID is a technology that for half a century has been used in a variety of ways.

RFID is, for example, used for managing library inventories, tracking cattle to prevent disease outbreaks, and for managing complex inventories in national retail chains.

RFID is also being used in other ways: in new easy-swipe credit cards, by California transit systems to collect fares, by federal and state governments in employee IDs and, perhaps best known, in new electronic passports for secure international travel.

When governments have considered the use of RFID for government-issued identifications, they have wisely avoided one-size-fits-all approaches to dealing with security and privacy issues. Where security is concerned, different government agencies will have different needs. A secure nuclear military base will require higher levels of security than a building open to the general public.

The same is true with safeguarding the privacy of the identification holder. Different approaches make sense depending on what could potentially be skimmed from the RFID. If the identification contains information traditionally considered to be identifying – Social Security Numbers (SSN), for example – governments have and should consider greater protections than if a simple random integer is used.

Thus, government properly uses a variety of different approaches to RFIDs. Where the passport is concerned, the federal government decided that if it was going to store the printed booklet information to a chip inside the cover and they would secure it with chip-based passwords and anti-counterfeiting and anti-tampering features.

Identification documents used for other purposes may warrant less security. Moreover, to speak of RFID as if it is a single uniform technology is to ignore the different ways it can be and has been deployed, in settings ranging from tracking inventory to passports.

The key point to make is that the technology itself can and should be proportionally scaled to safeguard data stored on the chip, based on the level of risk that personal information could be compromised and the cost of protecting against that risk.

The key observation about this key point is that it properly requires highly situational risk and benefit analyses. One-size-fits-all legislative solutions specifically targeting RFIDs are for this reason likely to be either over-inclusive or under-inclusive. They may be over-inclusive by requiring more protection than is actually needed in a particular situation, thus making the RFID cost prohibitive and leaving government procurement officials with existing options that may be less protective than the RFID (see discussion below). Or, they may be under-inclusive because the minimum privacy protections prescriptively required by the legislation will functionally also become the maximum protection afforded, and the protection mandated may be too little given the sensitivity of the data.

B. Demystifying RFID -- Everything Old Is New Again

Several of the recent RFID-related legislative proposals have sought to classify random unique identifiers – usually a random integer – as personally identifiable information. More than anything else, this in our opinion reveals how apprehensions about RFID are, respectfully, misplaced.

Consider the license plate on the back of your car. The license plate identifier is accessible by anyone from a vast distance, is unencrypted and otherwise unprotected, and is used routinely by law enforcement and businesses without warrants or other due process.

This unique number-letter identifier is stored in the DMV database that also contains personal information.

Yet, no privacy advocate has ever sought legislation requiring that the license plate unique identifier be visually obfuscated, obscured, or otherwise made invisible. Indeed, it is actually against the law to try and obscure it.

True, people other than the owner of the car could be driving or riding the car, but a government issued RFID identification could also be handed to a third party.

In any case, the reason no such bill has been introduced is because it is widely – if tacitly – understood that this unique number-letter string in and of itself cannot actually identify anyone. It is understood by the public and policymakers that what poses a risk to privacy is not someone seeing the unique identifier alone – it is just a string of random numbers and letters with no inherent nexus to anyone. Rather, it has always been understood that the security of the database that links the unique identifier to personally identifiable information is properly the focus of privacy concerns.

Phrased another way, there is no difference where privacy is concerned between a unique license plate identifier that is accessible by plain sight to millions that can be linked to databases containing personally identifiable information and a unique, random RFID identifier also linked to such a database, except that, because RFID is not visible to the naked eye and requires a special reader that needs to be "awakened", RFID is far more secure.

Hence -- and this is the essential point here -- the mere fact that information – even personal information -- may be carried via radio frequencies and become potentially

accessible to third parties does of course pose privacy challenges, ***but it does not pose new privacy challenges.*** Indeed, this is the oldest privacy challenge. Telephones, telegrams, billboards, email, bulk "snail" mail, printing – ***any means by which information can be conveyed to many people can also convey personally identifiable information to many people, thus posing a risk to privacy.***

For example, it wasn't so long ago that some states used SSNs as their driver's license numbers, with the SSN displayed on the license. Likewise, as late as the mid 1990s law schools would use the SSN as a student's exam number and post grades in public places using those numbers.

Yet no one has confusingly approached these poor practices as being the fault of a particular technology. The same is true of email, telephones, billboards, and off-set printing (to name just a few). These technologies, like "RF", are neutral ways to convey information and whether the information is conveyed via light waves, as is the case when someone looks at a SSN on the front of a driver's license, or radio waves, as is the case with RFID, the challenges are in the main the same.

Therefore, what separates the parties in the RFID debate is not whether there are privacy challenges posed by RFID. Every form of communication carries with it the risk that private information can be communicated. And that risk rises to the extent that information inherently capable of being tethered to an individual – true personal information -- is both used and accessible. RFID is no exception.

Rather, what separates the parties is whether those challenges are unprecedented warranting unprecedented legislative micro-management dictating to government agencies how they must procure an evolving, potentially beneficial technology that can be used in a variety of ways in a variety of settings.

What has prevented the license plate number from becoming a privacy risk? Was it a mandate that only certain types of technology be used in their manufacture? What prevents companies from printing SSNs on letterhead? Is it a law that regulates the manufacture of printing presses?

No. What has protected the unique identifier on the back of our cars from becoming the equivalent of SSNs is ***how it is used***. Likewise, no law regulates the design of printers to block the printing of SSNs. Billboard owners are not by law required to alter the materials of their billboards just because someone could post personal information on them.

What prevents the privacy problem from arising is how we use the personal information not the capability of the technology in and of itself to be used foolishly.

Of course, there are limits to the license plate-unique identifier hypothetical. Thus, if in some dystopian future, we were forced to tattoo a unique identifier on our foreheads, specific protections would likely (hopefully) be insisted upon.

But refinements to hypotheticals leading to different possible protections only underscore our main point in this testimony. It is the precise use of the technology – not the technology itself -- that matters; that dictates the level of security wisely required. Small changes in the hypotheticals can lead to different prescriptions.

Thus, put a unique identifier on the back of your car, no protection. Put the same ID on your forehead, protection. Put it on a tee-shirt that can be taken off or given to someone else... who knows? We will want to match protection precisely with exact kind of threat -- and that is why one-size-fits-all legislation is misguided.

The chip just sits there. It is a chip. How it is used, what information is on it, how far it can transmit, what it will be used for, what protections are therefore properly required, these are all problems that are properly focused on what people do and the context within which they are doing it.

For all these reasons, AeA would not in concept oppose efforts that addressed prohibited uses. Examples include:

- Efforts to address the potential unauthorized use of random identifiers by entities that did not issue the identifier.

- Efforts to address the use of SSNs, name, address, email addresses, telephone numbers, or driver's license numbers from being transmitted via a RFID-capable identification unless such information is protected.

- Strong criminal and civil penalties against those third parties or persons who inappropriately seek to remotely scan a person's identification document.

But what is anathema to AeA and its many member companies – even the vast majority that do not manufacture or sell RFID products -- are legislative solutions that try to react to legitimate privacy fears but, in doing so, first misapprehend the true cause of those concerns, blaming a technology for problems caused by people, and, second, that will result in the distortion of technological evolutions that might if left alone benefit both consumers and businesses.

C. The Necessity Of Comparisons.

It is in our opinion disingenuous to discuss the privacy challenges of any particular technology without an accompanying and honest assessment of the vulnerabilities of the existing alternatives. Thus, to discuss the vulnerabilities of RFID without also weighing the vulnerabilities of bar codes, magnetic strips, biometrics, passwords, and guards looking at a photo ID is to erect a massive straw man where, because RFID is legislatively approached in isolation, the misimpression is created that it is riskier than those technologies not discussed.

The possible consequences of legislative micro-managing RFID must fairly be assessed from the perspective that, if its use were discouraged, less secure alternatives may be the only options left standing, to the detriment of Californian's privacy.

No means of identification is hacker-proof or foolproof. The fact that a particular technology can, with determination and in a laboratory-like setting, be compromised only proves that it is a man-made technology. What should matter to privacy advocates is the relative ease with which various technologies can be compromised.

Thus, policymakers, business executives, and procurement officials must – if their efforts are to be credited as ones based on facts – ponder and address RFID contextually, always asking whether if used wisely it is more or less secure than the others, used with comparable wisdom.

D. Proposed RFID Legislation

In 2006, four bills were introduced in California to prohibit various state or municipal entities within California from issuing identification documents that contain a contactless integrated circuit (or RFID enabled computer chip), which would allow for the remote scanning of data contained on the chip; ultimately, these bills failed. In the 2007 legislative session, five new bills have been introduced which inappropriately address RFID technology instead of promoting the appropriate use of the technology.. Five of these new bills were introduced by Senator Joe Simitian, SB 28, SB 29, SB 30, SB 31, while Senator Ellen Corbett introduced SB 388.

AeA opposed all of these bills. While there are various specific reasons supporting its opposition unique to each measure, thematically AeA objected (i) to the singling out of RFID for targeted legislation apart from a broader approach that treated RFID the same as any other means of identification; and (ii) that the approach to many of them was to try and regulate the technology itself rather than setting parameters for the wise an unwise use of the technology by people.

Identification credentials (RFID enabled) are a technology that can play a strong role in protecting consumer's personal information which is why, for example, major multi-national financial institutions with vast financial and litigation exposure are moving to RFID-enabled credit cards.

The levels of security RFID chips provide can provide a more effective protection from theft and duplication of identity information, thereby reducing the opportunities for fraud in ID documents and the government programs accessed by these documents. RFID enabled chips can and are being safely used in a number of different privacy-sensitive areas such as financial transactions and healthcare/hospital environments – and even in secure identity documents.

RFID technology has been in use for more than 50 years and is in more than 1.3 billion identification credentials worldwide without a single documented case of harm or identity theft.

These are simply facts. The many, many companies now moving to RFID are in part doing so because it is more secure than the technological alternatives curiously never mentioned or admonished by privacy advocates. These companies are not in the habit of fiscal or public relations suicide. If they are at great expense and at some risk moving to RFID it is fair to infer that it is because they – at the very least – do not perceive the technology as any more risky than the alternatives.

E. AeA Recommended Best Practices

AeA stands in strong support of Californian's right to privacy. We believe that privacy is best protected by best practices designed to secure personal identification data from theft and exploitation. Technology's role is to implement those best practices to protect and expand consumer privacy. To this end, AeA has broadly laid out general privacy principles applicable to all situations where privacy may be at-risk:

- *Privacy & Security Policies*: Any organization that collects personal information must have strong policies in place that tells what information is collected, how it is stored, who has access to it, and how it will be protected.
- *Accuracy & Integrity*: When an individual is given an identity document that contains RFID, strict care must be taken to ensure that all information is accurate, as well as held strictly confidential.
- *Security, Security, Security*: All personal information must be protected at all times, from the moment of collection, while being stored, and even when in use. No exceptions.
- *The ID Must Be Secure As Well:* The identity document needs to protect its personal information from being copied, altered or hacked, to prevent unauthorized use, misuse, or disclosure of any personal information it carries.
- *Protected Exchange of Information:* Transferring personal information between the ID and the reader must be safeguarded against the unauthorized capture of information.
- *Authorized Access to Information:* Access must only be granted to those whom the issuer deems necessary and the personal information released should be only to authorized persons or systems.
- *Internal Commitment to Security:* Anyone using the system must be trained and monitored to ensure that all the security policies and practices put in place are adhered to.

All of these policies together represent a sliding scale of privacy protection. The more personal the information – the more it inherently can be used to identify a particular individual – the greater the protection that should be considered. But, to observe that the neighborhood bank has fewer protections than Fort Knox is not to indict the neighborhood bank as insecure requiring legislative micro-management of bank architecture. Each must be assessed and judged situationally, based on an assessment of use and hence risk.

And to reiterate: This is precisely why one-size-fits-all legislative proposals that seek to mandate particular technological solutions to protect privacy are poor public policy, for if they are to be practically achievable when enacted, they must be some form of lowest common denominator. This, in turn, means that in some situations the law will have codified and hence blessed as adequate privacy protections that are in fact inadequate the very moment they are written into law. At the same time, such a law will potentially discourage investment money from flowing into new, different, but not legally blessed technologies that might have been far more protective than the options we have now.

D. Summary

A technology that has never been breached for identity theft in more than half a century of use; that is potentially more secure than competing technologies; that is being increasingly used by conservative, risk-averse major companies and government agencies in light of the proven vulnerabilities of other comparable approaches; that, at bottom, is merely a way to communicate information and thus is no more inherently suspect than a printing press, billboard, radio, television, or telephone; this technology simply does not warrant the intense scrutiny it has dubiously enjoyed recently. There are privacy challenges in the use of RFID to be sure but they are the same challenges that arise whenever a technology makes it easier for people to communicate private facts to many other people.

Respectfully submitted: AeA,
October 31, 2007
Sacramento, California